

ABSTRACT OF THE DISCLOSURE

A stream 14 of external computer program calls made from an application program 2 to an operating system 4 is logged by an anti-malware layer 8. This stream 14 is examined for a primary set XYZ of external program calls known to be associated with malicious computer program activity. When such a primary set XYZ of external computer program calls is identified, the malicious activity is blocked and the logged stream 14 is examined to determine one or more secondary sets of external program calls which are now added to the set of rules 10 against which the logged stream 14 of external program calls is tested. In this way the set of rules 10 is dynamically adapted so as to more rapidly and proactively identify malicious computer program activity.

[Figure 2]